Recent Case Report

U.S. v. Buckner

(4th Cir. 2007) __ F.3d __ [2007 WL 64268]

ISSUES

Did officers reasonably believe that the defendant's wife could consent to a search of a computer in the family's living room?

FACTS

Officers in Virginia were investigating several complaints about online fraud committed by someone using AOL and eBay accounts in the name of Michelle Buckner. While meeting with Michelle in her home, officers noticed a computer in the living room. They could see that the computer was on because the screen was "lit." After explaining that she had leased the computer, Michelle gave the officers permission to remove the hard drive for a forensic search. Michelle's husband, Frank, was not home at the time.

The officers cloned the hard drive, then searched it by means of forensic search software. Some of the files they accessed had been created by Frank, and these files contained incriminating evidence that was used against him at his trial on charges of wire fraud. He was convicted.

It turned out that these files had been password protected by Frank, and that Michelle did not know the password. In other words, Frank was the only person who could access them. Michelle did not, however, inform the officers of this. Furthermore, the officers' search software automatically examined *all* files, regardless of whether they were password-protected.

DISCUSSION

Buckner contended that the information in the files should have been suppressed because, (1) Michelle lacked authority to consent to the search; and (2) even if she had authority, she could not consent to a search of files that were accessible only to him.

It is settled that a suspect's spouse may consent to a search of a place or thing owned or controlled by the suspect if the spouse had "actual authority" to give consent. As a general rule, a person has actual authority if she had "joint access or control" over the place or thing.[1]

[1] See *Illinois* v. *Rodriguez* (1990) 497 U.S. 177; *United States* v. *Matlock* (1974) 415 U.S. 164, 170-1; *People* v. *Welch* (1999) 20 Cal.4th 701, 748.

The problem here was that Michelle could not have accessed Frank's password protected files, which meant she did not have actual authority.[2] As the court explained, "Michelle Buckner did not have actual authority to consent to a search of her husband's password-protected files because she did not share mutual use, general access or common authority over those files."

It is also settled, however, that a search authorized by a person who, it was later determined, did not have actual authority will be upheld if officers reasonably believed she had it. To put it another way, the search will be upheld if the consenting person had "apparent authority." As the United States Supreme Court explained, "[D]etermination of consent to enter must be judged against an objective standard: would the facts available to the officer at the moment warrant a man of reasonable caution in the belief that the consenting party had authority over the premises?"[3]

In applying this rule, the court concluded that the officers reasonably believed that Michelle had authority to consent to a search of the hard drive because, (1) they knew she had leased the computer, (2) the computer was located in a "common living area" of the Buckner's home, (3) the computer was on even though Frank was not present, and (4) they had been told that fraudulent activity had been conducted from the computer using accounts opened in *Michelle's* name."

Consequently, the court ruled the search was lawful.

COMMENT

The question remains: What if the officers had known beforehand that Frank's files were password-protected? Would this have meant the files could not have been searched pursuant to Michelle's consent? This was not an issue because the officers utilized forensic software that automatically read and searched *all* files—even those that were password-protected. Furthermore, the court noted that "[e]ven during the mirroring and forensic analysis processes, nothing the officers saw indicated that any computer files were encrypted or password-protected."

The court indicated, however, the search might have been unlawful if the officers had deliberately kept themselves uninformed by making sure that the software they used would *not* notify them that they were about to access password-protected files. POV

[2] See *Trulock* v. *Freeh* (4th Cir. 2001) 275 F.3d 391, 403 ["Although Conrad had authority to consent to a general search of the computer, her authority did not extend to Trulock's password-protected files."].

[3] *Illinois* v. *Rodriguez* (1990) 497 U.S. 177, 188.